UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,793	04/13/2001	Jung-Wan Ko	1293.1191	1932

21171 7590 01/27/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Offic Action Summary	**Application No.** 09/833,793	**Applicant(s)** KO ET AL.	
	Examiner Ponnoreay Pich	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the c   ver sheet with th   correspondence address --

Peri d f r Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _13 April 2001_.

2a)□ This action is **FINAL**.   2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-45_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-45_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _4/13/2001_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 1-45 have been examined and are pending.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 00-31028, filed on 06/07/2000.

Information Disclosure Statement

The examiner has considered document number 9-200196. The examiner has not considered document titled "Japanese Office Action" as the examiner does not know how to read Japanese and no certified English translation was provided by the applicant.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 12-15, 29, 35, and 43-45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 12 recites the limitation "the transmitted cipher text" in line 2. There is insufficient antecedent basis for this limitation in the claim.
2. Claim 13 recites the limitation "the second encryption key" in lines 34. There is insufficient antecedent basis for this limitation in the claim.

3. Claim 13 recites the limitation "the transmitted first encryption key" in lines 7-8. There is insufficient antecedent basis for this limitation in the claim.
4. Claim 13 recites the limitation "the transmitted region segmentation information" in line 8. There is insufficient antecedent basis for this limitation in the claim.
5. Claim 13 recites the limitation "the transmitted second encryption key information" in line 10. There is insufficient antecedent basis for this limitation in the claim.
6. Claim 13 recites the limitation "the second region of the cipher text" in line 11. There is insufficient antecedent basis for this limitation in the claim.
7. Claim 13 recites the limitation "the extracted second encryption key" in line 11-12. There is insufficient antecedent basis for this limitation in the claim.
8. Claim 29 recites the limitation "the encrypted first and second portions" in line 2. There is insufficient antecedent basis for this limitation in the claim.
9. Claim 35 recites the limitation "the first region of the text" in 1-2. There is insufficient antecedent basis for this limitation in the claim. The examiner assumes the applicant meant to state “the first region of the encrypted text”.
10. Claim 35 recites the limitation "the second region of the text" in line 2. There is insufficient antecedent basis for this limitation in the claim. The examiner assumes the applicant meant to state “the second region of the encrypted text”.

11. Claims 43, 44, and 45 recite the limitation "the sender" in line 1 of each claim respectively. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6, 13-15, 18, 22-23, 30-31, and 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al (U.S. 5,761,311).

1. Claims 1 and 18: Spelman et al disclose an encryption method wherein a message is divided into multiple parts/blocks and at least one of those parts have a secondary encryption key, k2, that is located within one of the message blocks and both the key, k2, and the message block is encrypted using yet another key, R. The key, k2, was used to encrypt another message block (abstract). Spelman et al further disclose transmitting a cipher text comprising these regions to another party (col 2, lines 13-25).

   Spelman et al do not explicitly disclose a copy protection method comprising the division of a text into just two regions as the applicant's claim implies. However, one of ordinary skill in the art at the time of the applicant's invention would recognize that Spelman et al's invention is a more secure variation on the applicant's invention as Spelman et al divided the message into four blocks and employed a method similar to the applicant wherein one of the keys used is located in a part of the message to be transmitted, both of which are encrypted with a different key. One of ordinary skill would recognize that there may be no need to divide a message into as many parts and use as many keys as Spelman et al did and perhaps there is a need to only divide a message into two parts if encryption speed was more of a concern than better security as is the case in some networks.

Claim 18 disclose a computer readable medium encoded with processing instructions for implementing a method of claim 1. Spelman et al disclosed that their invention could be used with computers and computer readable mediums (col 4, lines 48-54).

2. Claim 13: Spelman et al as mentioned, disclose a method in which a message is divided into multiple blocks and each block is encrypted with a different key. At least one of those blocks, which is encrypted with a first key, contain another key, which is used to encrypt another block (abstract).

   Spelman et al do not explicitly disclose a copy protection method for decrypting a cipher text received from a sender who transmits the cipher text, the first encryption key, region segmentation information, and second encryption key information to a receiver, comprising:

   a. Decrypting the first region of the cipher text using a transmitted first encryption key and a transmitted region segmentation information.

b. Extracting the second encryption key from the decrypted first region using a transmitted second encryption key information.

c. Decrypting a second region of the cipher text using an extracted second encryption key.

However, as mentioned already, one of ordinary skill would recognize that the encryption method disclosed by Spelman et al is a more advanced variation on the method of the applicant's invention. One of ordinary skill would recognize that a sender who does the encryption must inherently send such information as a cipher text, the first encryption key, region segmentation information, and second encryption key information to a receiver, otherwise the receiver would not be able to decrypt the message. Further, one of ordinary skill would recognize that the decryption of a message is often the inverse process of encrypting the message. Therefore, as Spelman et al teaches information that can be used to encrypt a message in a manner similar to the applicant's invention, one of ordinary skill would be able to use Spelman et al teaching's to also decrypt a message in a manner similar to the applicant's invention.

3. Claims 6, 14, 23, and 34: Spelman et al do not disclose the copy protection method according to claim 1 and claim 14 and the computer readable medium according to claim 18 and claim 30 respectively, wherein a size of the first encryption key is fixed, and the size of the second encryption key is varied by a transmission unit within the first region. However, one of ordinary

skill would be motivated to do so as by fixing the size of the first encryption key, that information would not have to be transmitted to a receiving party via secure channel more than once if the receiving party was expected to receive multiple encrypted messages using the same encrypting method. This would save on the amount of network resources used by the system. By varying the size of the second encryption key by a transmission unit within the first region, one of ordinary skill would make the second key more secure, thus perhaps making up for the first encryption key not being as secure as its size is fixed.

4. Claim 15: Spelman et al do not explicitly disclose the copy protection method according to claim 13, wherein the first region of the text is smaller than the second region of the text, and a size of the first encryption key is larger than a size of the second encryption key.

However, one of ordinary skill in the art at the time the applicant's invention was made would recognize that there is a direct relationship between key strength, key size, and how long it would take to encrypt data using said key. As the first key is used to secure the second key, the first key need to be as secure as possible, therefore the first key size would be larger than the second key. As the second key is already secured by a strong first key, it does not need to be as large as the first key. Therefore, for fast encryption purposes, it would make sense to make the second region larger than the first as the second key can be used to encrypt large regions of data faster than the first key since its size is smaller.

5. Claim 22: Spelman et al do not disclose the computer readable medium of claim 18, wherein the second encryption key is smaller than the first encryption key. However, one of ordinary skill would recognize that as the first encryption key is being used to protect the second encryption key, the second one does not have to be as large as the first. A smaller second key would allow for faster encryption of the bulk of the message. In this manner, a compromise between security and encryption speed can be reached.
6. Claim 30: Spelman et al disclose that the methods of their invention can be used with a computer and a computer readable medium encoded with processing instructions for implementing the methods disclosed by Spelman et al (col 4, lines 48-54). Spelman et al further disclose decrypting an encrypted text sent between a sender and a receiver (col 2, lines 26-42).

Spelman et al neither explicitly disclose decrypting a first region of the encrypted text using a first encryption key, where the first region contains a second encryption key nor decrypting a second region of the encrypted text using the second encryption key. However, Spelman et al disclose an encryption method wherein a message is divided into multiple blocks and a second key is encoded into at least one of those blocks, which in turn is encrypted by another key. The second key is used to encrypt another block (abstract). One of ordinary skill would recognize that the decryption process is often the inverse of the encryption process. As the encryption process disclosed by Spelman et al is similar to that disclosed by the applicant, one of ordinary skill would recognize that to decrypt the message, one would need to decrypt the first region of the encrypted text using the first encryption key. Then, to decrypt the second region that was encrypted with the second key, one would need to use the second encryption key.

7. Claim 31: Spelman et al do not explicitly disclose a computer readable medium according to claim 30, wherein said decrypting the first region further comprises decrypting the first region using segmentation information and extracting the second encryption key from the decrypted first region using information related to the second encryption key. However, as stated, one of ordinary skill would recognize that decryption is often the inverse process of encryption, so would recognize that to decrypt the first region, one would need to decrypt the first region using the region segmentation information. Also, one of ordinary skill would recognize that the second key would need to be extracted from the decrypted first region using information related to the second encryption key, as the second key would be needed to decrypt the encrypted second region later.
8. Claim 35: Spelman et al do not explicitly disclose the computer readable medium according to claim 30, wherein a first region of the encrypted text is smaller than a second region of the encrypted text, and a size of the first encryption key is larger than a size of the second encryption key. However, one of ordinary skill would recognize that as the first encryption key is being used to keep the second key safe, its strength would need to be stronger than

the second, therefore its size would need to be larger. Further, as speed is a concern in encryption also, since the second encryption key is smaller, encryption using it would be faster, so as the second part of the message is encrypted using the second encryption key, it would make sense to make the second part of the message larger as this would allow encryption of the entire message to go faster.

Claims 2, 7-12, 16, 19, 24-29, 32-33, and 36-45 rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al (U.S. 5,761,311) in view of Lynn et al (U.S. 5,345,508).

1. Claim 2: Spelman et al disclose sending confidential information such as the method used to encrypt each parts of the message (col 2, lines 13-25).

   Spelman et al do not explicitly disclose that the confidential information comprises the first encryption key, region segmentation information for segmenting the text into the first region and the second region, and information related to the second encryption key. However, one of ordinary skill in the art would recognize that such information must be must inherently be sent to the intended recipient as the method to decrypt an encrypted message is often the reverse of the encryption process. Such information would be needed by someone who is intended to decrypt a message if they were to decrypt the message properly.

   Spelman et al do not disclose that the message was transmitted using a safe transmission path. However, Lynn et al disclose the transmission of confidential information such as a secret key through the use of a secure channel (col 1, lines 31-37). One of ordinary skill would recognize that it would do no good to encrypt a message and transmit how it was encrypted to an intended party if the method and key used for encryption were fall into the hands of a hacker, so one of ordinary skill would most likely use a secure channel when transmitting such information.

2. Claim 19: Spelman et al disclose sending confidential information such as the method used to encrypt each parts of the message (col 2, lines 13-25). Spelman et al also disclosed that their invention could be used with a computer readable medium (col 4, lines 48-54)

   Spelman et al do not explicitly disclose sending the first encryption key and information related to the second encryption key through a safe transmission path. However, one of ordinary skill would recognize that a receiving party would need the first encryption key and information related to the second encryption key to properly decrypt the message.

   Spelman et al also do not disclose that the message was transmitted using a safe transmission path. However, Lynn et al disclose the transmission of confidential information such as a secret key through the use of a secure channel (col 1, lines 31-37 and fig 1(a)). One of ordinary skill would recognize that it would do no good to encrypt a message and transmit how it was encrypted to an intended party if the method and key used for encryption were fall into the hands of a hacker, so one of ordinary skill would most likely use a secure channel when transmitting such information.

3. Claims 7 and 24: Spelman et al and Lynn et al do not disclose the copy protection method according to claim 2 and the computer readable medium according to claim 18 respectively, wherein the information related to the second encryption key includes size and position information of the second encryption key. However, as mentioned already, an decryption process is often the reverse of the encryption process, so one of ordinary skill would recognize that one would inherently need to send to a party who will be decrypting a message the information related to the second encryption key including the size and position information of the second encryption key.
4. Claims 8 and 25: Spelman et al and Lynn et al do not disclose the copy protection method according to claim 7 and the computer readable medium of claim 24 respectively, wherein the position and size information of the second encryption key are fixed. However, one of ordinary skill would be motivated to keep the position and size information of the second encryption key fixed as then that information would only be needed to be transmitted to a decrypting party once. This would save on network resources in networks where speed is more important than greater security.
5. Claims 9 and 26: Spelman et al and Lynn et al do not disclose the copy protection method according to claim 7 and the computer readable medium of claim 24 respectively, wherein the position and size information of the second

encryption key are varied. However, one of ordinary skill would be motivated to vary the size and position information of the second key as sometime greater security is more important than encryption speed or conserving uses of network resources.

6. Claims 10 and 27: Spelman et al and Lynn et al do not disclose the copy protection method according to claim 2 and the computer readable medium of claim 19 respectively, wherein the first region of the text is smaller than the second region of the text. However, one of ordinary skill in the art would be motivated to keep the first region of text smaller than the second region as the larger the region that must be encrypted with the first encryption key, the longer it would take to do the encryption. As the second encryption key is encrypted by a first encryption key, which one of ordinary skill would presumably choose to be stronger than the second encryption key, it would be faster to encrypt most of the message with the second encryption key than the first.
7. Claim 11: Spelman et al and Lynn et al do not disclose the copy protection method according to claim 2, wherein the region segmentation information comprises information on a starting address of the second region of the text. However, such information would be needed to decrypt an encrypted message properly, so the region segmentation information must inherently comprise information on a starting address of the second region of the text.

8. Claim 12: Spelman et al and Lynn et al do not disclose the copy protection method according to claim 2, further comprising:
    a. Decrypting the first region of a transmitted cipher text using the transmitted first encryption key and the transmitted region segmentation information.
    b. Extracting the second encryption key form the decrypted first region using the transmitted information related to the second encryption key.
    c. Decrypting the second region of the transmitted cipher text using the extracted second encryption key.

    However, one of ordinary skill in the art at the time of the applicant's invention would recognize that the method of decryption is often the exact reverse of the encryption method and would employ the decryption method as disclosed by claim 12.
9. Claim 16: Spelman et al and Lynn et al do not explicitly disclose the copy protection method according to claim 2, wherein the region segmentation information comprises information on a size of the first region of the text. However, the region segmentation information must comprise information on a size of the first region of the text, as this information is needed to decrypt the message properly.
10. Claim 28: Spelman et al do not explicitly disclose a computer readable medium according to claim 24, further comprising sending information on a starting address of the second region through the safe transmission path.

However, it would be obvious to one of ordinary skill in the art at the time of the applicant's invention to send such information as it would be needed to properly decrypt the message. Further, Lynn et al disclose that the use of a safe transmission path to transmit sensitive information was known at the time of the applicant's invention (col 1, lines 21-27 and fig 1(a)). One of ordinary skill would use the safe transmission path to transmit this needed information so that a hacker would not gain this information and more easily break the encryption.

11. Claim 29: Spelman et al do not explicitly disclose the computer readable medium according to claim 28, further comprising sending a cipher text comprising the first and second portions through an unsafe transmission path and obtaining the safe transmission path through authentication operations. However, Lynn et al disclose in fig 1(a) a cipher text message being sent over a public or unsafe transmission path. As the message is already encoded, one of ordinary skill would be motivated to send through the unsafe path as it would probably be faster and cheaper to do so. Neither Spelman et al nor Lynn et al disclose that the safe transmission path is obtained via authentication operations, but the examiner would like to use official notice to note that obtaining a safe path via authentication operations was well known at the time of the applicant's invention. One of ordinary skill would be motivated to make use of authentication operations to obtain a safe path as it is a simple and quick way of obtaining the safe path.

12. Claim 32: Spelman et al do not explicitly disclose the computer readable medium according to claim 31, wherein the region segmentation information, the region related to the second key, and the first encryption key are received through a safe transmission path. One of ordinary skill would recognize these information as needed for the decryption process. One of ordinary skill would further recognize that with these information it would be easier for a hacker to decrypt the message, so would be motivated to transmit the information via a secure path as disclosed by Lynn et al (col 1, lines 21-27 and fig 1(a)).
13. Claim 33: Spelman et al do not explicitly disclose the computer readable medium of claim 32, further comprising receiving the encrypted text through an unsafe transmission path. However, Lynn et al disclose sending a cipher text message through an unsafe path (col 1, lines 21-27 and fig 1(a)). One of ordinary skill would recognize that the message is already encrypted, so it might be faster to transmit the encrypted message using the unsafe path.
14. Claim 36: Spelman et al disclose a sender for sending encrypted text, comprising an encryptor to encrypt a text using an encryption key (col 2, lines 13-25). Spelman et al do not disclose an authenticator to obtain a safe transmission path through which a first encryption key and information related to a second encryption key are sent. However, the examiner would like to use official notice to note that an authenticator for obtaining a safe transmission path was known at the time of the applicant's invention. Further Lynn et al disclose the use of a safe transmission path to send sensitive data

such as an encryption key (col 1, lines 21-27 and fig 1(a)). Spelman et al also disclose an encryption method in which a text is divided into multiple blocks and encoded with different keys. At least one of those blocks is encoded with a first key and contains a second key (abstract). One of ordinary skill would recognize that one can take Spelman et al's teachings and arrive at the applicant's invention by just dividing the message into two portions instead of four as disclosed by Spelman et al. One of ordinary skill might want to do so for faster encryption.

15. Claim 41: Spelman et al disclose a receiver for sending encrypted text, comprising an encryptor to encrypt a text using an encryption key (col 2, lines 26-42). Spelman et al do not disclose an authenticator to obtain a safe transmission path through which a first encryption key and information related to a second encryption key are received. However, the examiner would like to use official notice to note that an authenticator for obtaining a safe transmission path was known at the time of the applicant's invention. Further Lynn et al disclose the use of a safe transmission path to receive sensitive data such as an encryption key (col 1, lines 21-27 and fig 1(a)). Spelman et al also disclose an encryption method in which a text is divided into multiple blocks and encoded with different keys. At least one of those blocks is encoded with a first key and contains a second key (abstract). One of ordinary skill would recognize that one can take Spelman et al's teachings and arrive at the applicant's invention by just dividing the message into two

portions instead of four as disclosed by Spelman et al. One of ordinary skill might want to do so for faster encryption.

16. Claims 37 and 42: Spelman et al do not disclose the sender of claim 36 and the receiver of claim 41, wherein the information related to the second encryption key comprises size and position information of the second encryption key and the encrypted text is sent/received through an unsafe transmission path. However, Lynn et al disclose an encrypted text being sent/received through an unsafe transmission path (col 1, lines 21-27 and fig 1(a)). One of ordinary skill might want to send through an unsafe transmission path as it would be faster to do so and the text is encrypted already, therefore secure. Lynn et al also do not disclose the information related to the second encryption key comprising size and position information of the second encryption key. However, it is inherent that the information comprise the size and position information as these information are needed to decrypt the message properly.

17. Claim 38 and 43: Spelman et al disclose the sender of claim 37 and the receiver of claim 42, wherein the sender/receiver comprises an information appliance (col 4, lines 47-54). Computers are inherently information appliances.

18. Claim 39 and 44: Spelman et al disclose the sender of claim 37 and the receiver of claim 42, wherein the sender/receiver comprises a computer (col 4, lines 47-54).

19. Claims 40 and 45: Spelman et al disclose the sender of claim 37 and the receiver of claim 42, wherein the sender/receiver comprises a server (col 4, lines 47-54). A server is inherently a computer.

Claims 3-5 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al (U.S. 5,761,311) in view of Seheidt et al (U.S. 5,787,173).

1. Claim 3: Spelman et al do not disclose the copy protection method according to claim 1, wherein the first encryption key comprises an encryption key for the use with a common key encryption method. However, Seheidt et al disclose that the use of symmetric keys for encryption was well known at the time of the applicant's invention by one of ordinary skill in the art (col 3, lines 31-46). Symmetric key encryption and shared key encryption are other names for common key encryption. One of ordinary skill would be motivated to use common key encryption method for the first encryption key as the encryption method is usually fast and can encrypt a large amount of data in a relatively short time frame. The examiner would like to note that the use of common encryption keys, though fast, is not as secure as other slower encryption methods, so when common encryption keys are used, encryption speed is usually more of a concern for the system.
2. Claims 4 and 21: Spelman et al do not disclose the copy protection method according to claim 1 and claim 19 respectively, wherein the first encryption key comprises a public/asymmetric key for use with a public/asymmetric key encryption method. However, Seheidt et al disclose that the use of public key

encryption was well known by one of ordinary skill in the art at the time of the applicant's invention (col 3, lines 4-31). One of ordinary skill would be motivated to use public key encryption for the first encryption key, as public key encryption is inherently more secure than common encryption keys, though encryption with it takes longer. One of ordinary skill would use public encryption keys where concerns for security far outweigh concern about encryption speed. The fact that public key encryption is typically slow, though strong was disclosed by Spelman et al also (col 8, last paragraph and col 9, 1st paragraph). Spelman et al disclosed that there are instances when it is more appropriate to use either public key or common key encryption over the other depending if one wanted speedier performance or greater encryption strength. The examiner would like to note that public keys are also known as asymmetric keys.

3. Claim 5: Spelman et al do not disclose the copy protection method according to claim 1, wherein the second encryption key is smaller than the first encryption key where a common key encryption key method is used. However, as mentioned already, one of ordinary skill would use a common encryption key for the first key when encryption speed is more of a concern than encryption strength. For this reason, one of ordinary skill would be motivated to make the second encryption key smaller than the first as this would further speed up the encryption process for any encrypting that needs to be done using the second encryption key.

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al (U.S. 5,761,311) in view of Seheidt et al (U.S. 5,787,173) and Ganesan et al (U.S. 5,588,061) .

1. Claim 17: Spelman et al do not disclose the copy protection method according to claim 3, wherein the larger first encryption key comprises an encryption key that is 56 bits or more. However, Ganesan et al disclose the use of an encryption key that is 56 bits or larger in size (col 6, 1st paragraph). One of ordinary skill would be motivated to use an encryption key that is 56 bits or larger for the first key as this would allow for greater encryption strength for the first key.

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spelman et al (U.S. 5,761,311) in view of Lynn et al (U.S. 5,345,508), Seheidt et al (U.S. 5,787,173) and Ganesan et al (U.S. 5,588,061).

2. Claim 20: Spelman et al disclose that their invention can be used with computers and computer readable mediums (col 4, lines 48-54). Spelman et al do no disclose the computer readable medium of claim 19, wherein the larger first encryption key comprises an encryption key that is 56 bits or more. However, Ganesan et al disclose the use of an encryption key that is 56 bits or larger in size (col 6, 1st paragraph). One of ordinary skill would be motivated to use an encryption key that is 56 bits or larger for the first key as this would allow for greater encryption strength for the first key.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. Dorenbos (U.S. 5,751,813) discloses a system where a message is encrypted twice with two different keys.
2. Katayanagi et al (U.S. 2001/0046296) disclose converting a plaintext into a ciphertext block by block, each block consisting of a predetermined number of bits.
3. Jakubowski et al (U.S. 6,226,742) disclose encrypting a message authentication code within the corresponding message block.
4. Mueller (U.S. 5,602,917) discloses symmetric key cryptography.
5. Easter et al (U.S. 5,559,889) disclose use of a public and private cryptographic key pair for encryption.
6. Merrick (U.S. 5,416,841) discloses use of keys 56 bits in length.
7. Fawcett, Jr. (U.S. 5,414,771) discloses encryption via use of a random key.
8. Orrin (U.S. 6,011,849) discloses encryption based on steganography in which an encryption key is both the key and the data to be encrypted.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100